REMARKS

Claims 1-21 are presented for further examination. Claims 9, 10, 13, 16, and 19 have been amended.

In the Office Action mailed February 21, 2007, the Examiner rejected claims 13-18 under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 4,887,296 ("Horne") in view of U.S. Patent No. 6,625,147 ("Yokoyama"). Claims 1-12 and 19-21 were rejected as obvious over Horne in view of U.S. Patent No. 6,728,379 ("Ishibashi") and further in view of Yokoyama.

Applicants respectfully disagree with the bases for the rejections and request reconsideration and further examination of the claims.

Claim 1 is directed to a circuit that utilizes an encryption layering scheme in which encrypted broadcast signals are decrypted using control signals. The control signals are received in encrypted form and decrypted using a common key. The common key is also received in an encrypted form and decrypted using a secret key.

One feature of the circuit recited in claim 1 is that there is a secure route for placing the common key in a key store and for providing decrypted control signals to a processing unit. More particularly, claim 1 specifies that "the only route to placing a common key in the common key store is to input the common key in encrypted form for decryption in accordance with the secret key and the only route to providing the control signals to the processing unit is to input them in encrypted form for decryption in accordance with the common key."

A second feature of the circuit defined in claim 1 is that all components are placed on the same integrated circuit, eliminating vulnerable interfaces that occur in previous smart-card based designs. For example, claim 1 specifies "a semiconductor integrated circuit… comprising…."

Horne describes an encryption layering scheme, but Horne is completely silent as to the precise circuit layout used. Therefore, this reference does not teach or suggest the central features recited in claim 1 wherein all components are provided on the same integrated circuit and providing secure routing of sensitive data (such as control signals and cryptographic keys) so that the data is not exposed at any vulnerable interface. Horne was filed in 1987, at a time when smart-card based systems were typical. In smart-card based systems, a vulnerable interface exists between the smart-card and smart-card reader. For this reason, in the absence of details in Horne as to the circuit layout, secure routing of sensitive data is not guaranteed, unlike the present claimed circuit.

Horne describes a transmitter that transmits encrypted data and an encrypted common key to a receiver that decrypts the common key using a stored individual key, and then uses the decrypted common key to decrypt the encrypted data. Horne does not teach or suggest having control signals that are transmitted in encrypted and decrypted with the common key.

The Examiner has applied the Yokoyama reference, asserting that it discloses decrypting control signals with a common key to generate decrypted control signals. The Examiner has further relied upon the Ishibashi reference as allegedly disclosing placing a common key in a common key store. However, there is no teaching in either of Yokoyama or Ishibashi, taken alone or in any combination therewith or with Horne, of secure routing of cryptographic keys and control signals in an integrated circuit in which vulnerable interfaces are eliminated.

Rather, Ishibashi describes an information processing method that prevents illicit copying of content data. Ishibashi actually teaches away from a central feature of the present claimed circuit inasmuch as illustrated for example in Figure 8, the cryptographic keys are stored in a hard disc (*e.g.*, hard disc 110) and transmitted to an encryption circuit. This arrangement must involve an insecure interface between the hard disc and the cryptographic processor since hard disc drives are not components integrated onto circuits. This creates a weakness in the overall security of the system not present in the claimed circuit.

Yokoyama describes a communications network control system capable of dispersing a processing load by separating a network control function from a packet transfer function. As such, it not relevant to the concept of securely routing cryptographic keys and a control signal in a circuit in which an encryption layering technique is employed. Even if one were motivated to combine the references in the manner suggested by the Examiner, the combination would not achieve the claimed circuit. For example, Yokoyama teaches using an unencrypted common key at both ends. In addition, Yokoyama does not teach using the control signals to decrypt encrypted data. Hence, the combination of Horne and Yokoyama would not be capable of decrypting the encrypted data using the decrypted control signals.

For these reasons, applicants respectfully submit that claim 1 is clearly allowable over the references cited and applied by the Examiner.

Dependent claims 2-8 are also allowable for the features recited therein as well as for the reasons why claim 1 is allowable.

Independent claims 9, 10, 13, 16, and 19 have all been amended to recite the features discussed above with respect to claim 1. Applicants respectfully submit that these independent claims as well as dependent claims 11, 12, 14, 15, 17, 18, 20, and 21 are all allowable for the reasons discussed above with respect to claims 1-8.

In view of the foregoing, applicants respectfully submit that all of the claims in this application are in condition for allowance. In the event the Examiner finds minor informalities that can be resolved by telephone conference, the Examiner is urged to contact applicants' undersigned representative by telephone at (206) 622-4900 in order to expeditiously resolve prosecution of this application. Consequently, early and favorable action allowing these claims and passing this case to issuance is respectfully solicited.

The Director is authorized to charge any additional fees due by way of this Amendment, or credit any overpayment, to our Deposit Account No. 19-1090.

Respectfully submitted,

SEED Intellectual Property Law Group PLLC

/E. Russell Tarleton/
E. Russell Tarleton
Registration No. 31,800

ERT:jl

701 Fifth Avenue, Suite 5400
Seattle, Washington 98104
Phone: (206) 622-4900
Fax: (206) 682-6031